(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－510970
（P2001－510970A）
(43)公表日　平成13年８月７日(2001.8.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04Q 7/38		H04B 7/26	109R	5J104
H04L 9/08		H04L 9/00	601B	5K067
H04Q 7/10			601A	
7/20			601E	
7/22		H04Q 7/02	Z	

審査請求　未請求　予備審査請求　有　（全 41 頁）　最終頁に続く

(21)出願番号　特願2000－503671(P2000－503671)
(86)(22)出願日　平成10年７月13日(1998.7.13)
(85)翻訳文提出日　平成12年１月17日(2000.1.17)
(86)国際出願番号　ＰＣＴ／ＧＢ９８／０２０６４
(87)国際公開番号　ＷＯ９９／０４５８３
(87)国際公開日　平成11年１月28日(1999.1.28)
(31)優先権主張番号　９７１５０９７．３
(32)優先日　平成９年７月17日(1997.7.17)
(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　オレンジ　パーソナル　コミュニケイションズ　サーヴィシーズ　リミテッド
イギリス，　ブリストル　ビーエス12　4キュージェイ，　アーモンズベリー，　グレート　パーク　ロード，　セイント　ジェイムズ　コート　（番地なし）
(72)発明者　フォード，　ピーター
イギリス，　ブリストル　ビーエス17　5アールピー，　イエイト，　サマーズ　ミード　18
(74)代理人　弁理士　山田　行一　（外２名）

最終頁に続く

(54)【発明の名称】　セルラー方式通信システムにおける暗号化同報メッセージ

(57)【要約】
所定のアクセス権を有するユーザ移動局（８）が、セルラー方式電気通信ネットワーク内の共通のセルチャネルで同報されたメッセージを明瞭に表示できるようにする方法を開示する。メッセージは、同報前に予め定められた暗号化キーを用いて暗号化され、対応する解読キーが対応するアクセス権を有する移動局（８）に与えられる。適切なアクセス権を欠いた移動局の場合、メッセージが受信されて取り上げられると、そのメッセージは、暗号化形式、すなわち理解できない形式でしか表示されない。同じ共通チャネル上のセル内で同報されるある種のメッセージは、一般アクセスメッセージとみなされる。この種のメッセージは、非暗号化形式で同報され、メッセージが同報されるセルにキャンプオンされた移動局（８）によって理解可能な形式で表示することができる。

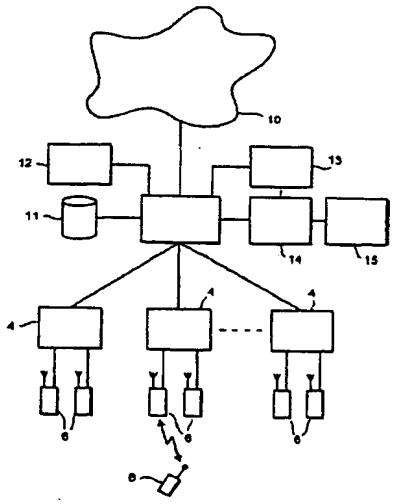


FIG. 1

【特許請求の範囲】

【請求項１】　セルラー方式電気通信ネットワークにおいてユーザに情報を配信する方法であって、前記ネットワークは、移動交換センタと、前記ネットワークの複数のセルにおいて送受信を行う複数の基地局と、を備えており、

複数の移動局を用意するステップであって、前記移動局の各々が、関連付けられた情報アクセスステータスを有しているステップと、

前記ネットワークの少なくとも一つのセルの共通チャネル上で信号を同報するステップであって、前記信号が、前記少なくとも一つのセルにおける一般受信のために、暗号化形式のアクセス制限メッセージを含んでいるステップと、

第１情報アクセスステータスを有する第１移動局が、前記メッセージを解読し、前記セルによりサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供できるようにするステップと、

第２情報アクセスステータスを有する第２移動局が前記セル内でサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供することを防止するステップと、

を備える方法。

【請求項２】　前記第１移動局に前記メッセージ用の解読キーが供給される請求項１記載の方法。

【請求項３】　前記解読キーが、複数の移動局のいずれかと関連付けて使用することの可能な着脱自在モジュール内に保持される、請求項２記載の方法。

【請求項４】　前記メッセージが前記着脱自在モジュールで解読される請求項３記載の方法。

【請求項５】　前記信号が、前記メッセージの一部分に付随するパディングデータを含み、この部分が非暗号化形式で前記信号に含まれる、請求項２または３記載の方法。

【請求項６】　前記信号が、メッセージに付随するメッセージ識別子を含むヘッダ部を備えており、前記第１および第２移動局の双方が前記メッセージ識別子を読み取ることができるようにするステップを備えている、請求項１～５のいずれかに記載の方法。

【請求項７】　前記情報アクセスステータスを定義するステータスデータが第１移動局の着脱自在モジュール内に記憶される請求項１～６のいずれかに記載の方法。

【請求項８】　前記ステータスデータが解読キーを含んでいる請求項７記載の方法。

【請求項９】　前記解読キーが前記着脱自在モジュール内に暗号化形式で記憶される請求項８記載の方法。

【請求項１０】　前記解読キーが、前記着脱自在モジュールに特有のデータ列を用いて前記第１移動局により解読される、請求項９記載の方法。

【請求項１１】　前記データ列が前記セルラー方式電気通信ネットワークで使用される加入者識別子である請求項１０記載の方法。

【請求項１２】　前記セルラー方式電気通信ネットワーク内で無線インタフェースを介して前記第１移動局に前記ステータスデータを送信するステップを更に備える請求項７～１１のいずれかに記載の方法。

【請求項１３】　前記信号が、対応するアクセス権を各々が有する複数のアクセス制限メッセージを含んでおり、

前記移動局に前記アクセス権を与えるステップと、アクセス制限メッセージに対応するアクセス権を有する移動局のみが、前記セル内でサービスが提供されるときにユーザにそのアクセス制限メッセージを提供できるようにするステップと、を備える請求項１～１２のいずれかに記載の方法。

【請求項１４】　前記第１移動局の各々に、各第１移動局に対して保有される加入契約に従って前記アクセス権のなかから選択されたものを提供するステップを備える請求項１３記載の方法。

【請求項１５】　複数のアクセス制限メッセージタイプの各々に対して暗号化キーを記憶するステップと、その対応メッセージタイプに応じた暗号化キーを用いて前記各アクセス制限メッセージを暗号化するステップと、を更に備える請求項１３または１４記載の方法。

【請求項１６】　複数の加入記録を記憶するステップを備え、前記加入記録の各々が前記アクセス権を定義するアクセス権データを含んでいる請求項１３～

１５のいずれかに記載の方法。

【請求項１７】　加入記録に対する前記アクセス権データを変更して、ユーザが理解可能なように受信することができるアクセス制限メッセージのタイプを変更するステップを備える請求項１６記載の方法。

【請求項１８】　前記信号が一般アクセスメッセージを含んでおり、前記第１および第２移動局の双方が、前記セル内でサービスが提供されるときに前記一般アクセスメッセージをユーザに提供できるようにするステップを備えている請求項１～１７のいずれかに記載の方法。

【請求項１９】　前記共通チャネルがＧＳＭ型通信システムのセルブロードキャストチャネルである請求項１９記載の方法。

【請求項２０】　他のアクセス制限メッセージが前記セルラー方式電気通信ネットワークの異なるエリアに位置するセル内で同報される請求項１～１９のいずれかに記載の方法。

【請求項２１】　セルラー方式電気通信システムにおいて情報を受信する装置であって、

解読キーを記憶する手段と、

前記セルラー方式電気通信システムのセルの共通チャネル上で同報されるメッセージを受信する手段と、

記憶された前記解読キーを用いて前記メッセージを解読する手段と、

解読された前記メッセージをユーザに対して表示する手段と、

を備える装置。

【請求項２２】　前記記憶手段が着脱自在モジュールの一部である請求項２１記載の装置。

【請求項２３】　前記表示手段は、前記メッセージに対する解読キーが前記記憶手段内に保持されているときに、メッセージを解読された形式で表示し、前記メッセージに対する解読キーが前記記憶手段内に保持されていないときに、前記メッセージを暗号化された形式で表示するように構成されている請求項２１または２２記載の装置。

【請求項２４】　前記解読手段が着脱自在モジュールの一部である請求項２

１、２２または２３記載の装置。

【請求項２５】　セルラー方式移動体電話である請求項２１、２２、２３または２４記載の装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＧＳＭ（Global System for Mobile communication：世界移動通信システム）ディジタルセルラー方式無線ネットワークなどのセルラー方式電気通信ネットワークにおける情報の配信および受信を行う装置の方法に関する。

【０００２】

【従来の技術】

ＧＳＭ標準は、欧州電気通信標準化機構（ＥＴＳＩ）発行の一組の技術仕様書に定義されている。現在では、ＧＭＳ標準、およびその変形例（例えばＤＣＳ１８００標準）に従って動作する多くの移動体電気通信ネットワークが存在する。

【０００３】

提供される一つのサービスは、セルブロードキャスト（ＣＢ）サービスまたはショートメッセージセルブロードキャスト（ＳＭＳ ＣＢ）サービスと呼ばれるサービスである。このサービスでは、テキストページ形式の情報が、ネットワーク内のセルの共通チャネル（セルブロードキャストチャネル、ＣＢＣＨ）で送信される。これらのページの送信は、一定間隔で繰り返される。ユーザは、移動局上でキーを選択操作して情報の検索および表示を行うために、その情報を保存することが可能であり、あるいはその情報を保存しないようにセルブロードキャスト機能をオフにすることができる。この情報は、地域施設（病院、薬局、タクシー等）のリスト、地域気象予報、地域日時表示など、地域特有の情報を含むように意図されている。

【０００４】

【発明が解決しようとする課題】

しかしながら、現在、セルブロードキャスト機能は、現行ＧＳＭ型ネットワークおよびそこで使用される移動局で提供されるものの、実際には広く実施されているわけではない。この理由の少なくとも一部は、おそらく、このサービスを介した情報の収集および配布に伴うコストである。

【０００５】

【課題を解決するための手段】

本発明のある態様では、セルラー方式電気通信ネットワークにおいてユーザに情報を配信する方法が提供される。ここで、このネットワークは、移動交換センタと、このネットワークの複数のセルで送受信を行う複数の基地局と、を備えている。この方法は、

複数の移動局を用意するステップであって、前記移動局の各々が、関連付けられた情報アクセスステータスを有しているステップと、

前記ネットワークの少なくとも一つのセルの共通チャネル上で信号を同報通信するステップであって、前記信号が、前記少なくとも一つのセルにおける一般受信のために、暗号化形式のアクセス制限メッセージを含んでいるステップと、

第１情報アクセスステータスを有する第１移動局が、前記メッセージを解読し、前記セルによりサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供できるようにするステップと、

第２情報アクセスステータスを有する第２移動局が前記セル内でサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供することを防止するステップと、を備えている。

【０００６】

本発明のこの態様の利点は、次の通りである。すなわち、情報へのアクセスを許可されていないユーザは、メッセージを暗号化形式でしか見ることができず、内容を理解することができない。一方、情報へのアクセス権を有するユーザは、解読済みの理解可能な形式でメッセージを見ることができる。サービスは、加入契約に基づいて提供することができる。ネットワーク中の一部の加入者は、電気通信ネットワークで提供される他のサービス（音声呼出しサービスなど）に加えてセル内で一般的に同報される情報にアクセスしたいと考えるかもしれず、その場合、セルラー情報同報サービスへのアクセスを可能にする加入契約を申し込むことになる。また、他のユーザは、セル内の情報同報の恩恵を受けたくないと考えるかもしれず、その場合、おそらくは少ない費用で、それらの情報へのアクセスを防ぐ加入契約を申込むことになる。

【０００７】

好ましくは、上記の信号は、対応するアクセス権を各々が有する複数のアクセス制限メッセージを含んでおり、上記の方法は、移動局にアクセス権を与えるステップと、アクセス制限メッセージに対応するアクセス権を有する移動局のみが、セル内でサービスが提供されるときにユーザにそのアクセス制限メッセージを提供できるようにするステップと、を備えている。これにより、ユーザがアクセス可能な情報の種類の選択がユーザ単位で可能となり、加入契約を加入者個々のニーズに適応させることが可能となる。

【０００８】

上記の信号は、一般アクセスメッセージを含んでいてもよく、上記の方法は、セル内でサービス提供されるときに第１および第２移動局の双方がユーザにその一般アクセスメッセージを提供できるようにするステップを備えていてもよい。これにより、アクセス制限メッセージおよび一般アクセスメッセージの双方をセルラー方式電気通信システムのセル内での同報により配布することが可能となり、保有する加入タイプにかかわらず、任意のユーザに情報を提供することが可能となる。

【０００９】

好ましくは、他のアクセス制限メッセージが、セルラー方式電気通信ネットワークの異なるエリアに位置するセル内で同報される。これにより、メッセージ内の情報を種々の地域に適合させ、サービスの有用性を高めることができる。

【００１０】

本発明の別の態様によれば、セルラー方式電気通信システムにおいて情報を受信する装置が提供される。この装置は、

解読キーを記憶する手段と、

前記セルラー方式電気通信システムのセル内の共通チャネルでメッセージを受信する手段と、

記憶された前記解読キーを用いて前記メッセージを解読する手段と、

この解読されたメッセージをユーザに対して表示する手段と、を備えている。

【００１１】

この態様は、ユーザが電気通信システム内の一つのセルの共通チャネルでアク

セス制限メッセージを受信し、ユーザの移動局に解読キーが与えられている場合には、解読された形式でその情報を見ることができるようにする装置を提供する。解読キーは、所定の加入タイプを有するセルラーユーザにのみ配布することができる。

【００１２】

【発明の実施の形態】

以下では、本発明の実施形態を添付の図面を参照しながら説明する。この実施形態は、単なる例示として記載したものにすぎない。

【００１３】

図１は、公衆陸上移動体ネットワーク（public land mobile network：ＰＬＭＮ）と呼ばれるＧＳＭネットワークを概略的に示している。これ自体は公知であるので、その詳細は省略する。移動交換センタ（mobile switching centre：ＭＳＣ）２は、通信リンクを介して多くの基地局コントローラ（base station controller：ＢＳＣ）４に接続される。ＢＳＣ４は、移動交換センタ２からサービスの提供を受ける複数のエリアにわたって地理的に分散される。各ＢＳＣ４は、一つ以上の基地トランシーバ局（base transceiver station：ＢＴＳ）６を制御する。このＢＴＳ６は、ＢＳＣから離れた場所に位置し、別の通信リンクを介してそのＢＳＣに接続される。各ＢＴＳ６は、ＢＴＳがサービスを提供するエリア内の移動局８との間で無線信号の送受信を行う。このようなエリアは、「セル」と呼ばれる。ＧＳＭネットワークには、このようなセルが数多く設けられる。これらのセルは、全ネットワーク領域にわたって連続したカバレッジを与えるように連続しているのが理想的である。無線信号は、多くの別個の通信チャネルに分けられる。これらの通信チャネルには、共通チャネルおよびトラヒックチャネルが含まれる。トラヒックチャネルは、特定の移動局とのポイントツーポイント通信（音声呼出し、データ呼出し等）に使用される。共通チャネルは、セルがサービスを提供する全ての移動局によって受信され、シグナリングデータおよび／又はメッセージデータを含んでいる。

【００１４】

移動交換センタ２は、通信リンクを介して、移動通信ネットワーク１０の残り

の部分における他の移動交換センタや、公衆加入電話網（public service telephone network：ＰＳＴＮ）等の他のネットワーク（図示せず）にも接続される。移動交換センタ２には、ホームロケーションレジスタ（home location register：ＨＬＲ）１１が設置される。ＨＬＲ１１は、各移動局８に対して一意の国際移動体加入者識別子（international mobile subscriber identity：ＩＭＳＩ）を含む加入者確認データを記憶するデータベースである。ＩＭＳＩは、移動体国番号（３桁の十進数）、移動体ネットワーク番号（２桁の十進数）、および特定ネットワーク内の加入者を識別する移動体加入者番号（最大１０桁の十進数）から構成されている。ＩＭＳＩは、加入者識別モジュール（ＳＩＭ）（後述する）内の移動局にも、他の加入者特有の情報と共に記憶される。

【００１５】

移動交換センタには、図示しないビジターロケーションレジスタ（ＶＬＲ）も設置される。ＶＬＲは、そのエリア内の移動局用の加入者確認データを一時的に記憶するデータベースである。

【００１６】

更に、ＭＳＣは、ネットワーク中でセルブロードキャスト（cell broadcast：ＣＢ）メッセージを発信するセルブロードキャストセンタ（cell broadcast centre：ＣＢＣ）１２、ネットワーク内のポイントツーポイントショートメッセージの転送を処理するショートメッセージセンタ（short message centre：ＳＭＣ）１３、ネットワーク内の管理機能を実行するネットワーク管理センタ（network management centre：ＮＭＣ）１４、およびシステム内のワークステーションでの手動入力による顧客加入データの更新などを含む顧客サービス機能を実行する顧客サービスシステム（customer services system：ＣＳＳ）１５に接続されている。

【００１７】

図２に示されるように、移動局８（より具体的には、セルラー方式移動体無線電話）は、送受信アンテナ１６、無線周波数トランシーバ１８、スピーカ２２およびマイクロホン２４に接続された音声CODEC２０、プロセッサ回路２６およびその関連メモリ２８、ＬＣＤ表示装置３０、並びに手動入力ポート（キーパッド

）３２を備えている。移動局８は、電気接点３５を介して、着脱自在なＳＩＭ３４に接続される。

【００１８】

移動局に接続されたＳＩＭ３４は、ＳＩＭプロセッサ３６（例えば、日立Ｈ８マイクロプロセッサ）およびＳＩＭメモリ３８を有する。ＳＩＭメモリ３８には、例えば、ＳＩＭオペレーティングシステムを含む１６キロバイトのマスクプログラムＲＯＭ３８ａ、データ項目の不揮発性記憶用の８キロバイト読み書きＥＥＰＲＯＭ３８ｂ、および動作中にＳＩＭプロセッサ３６によって使用される２５６バイトＲＡＭが含まれる。

【００１９】

上述のように、ＳＩＭ３４は、移動局８のプロセッサ２６によるデータ項目の記憶および検索に使用される。移動局プロセッサ２６およびＳＩＭプロセッサ３６間のインタフェースを介して通信されるデータに関するコマンドセット、データファイル構造およびデータ符号化フォーマットは、すべてＧＳＭ技術仕様書１１．１１に指定されている。

【００２０】

図１に示されるネットワーク要素に戻ると、ＣＢＣ１２は、ネットワーク内で同報されるべき一組のセルブロードキャストメッセージを保持し、各メッセージタイプに対して予め定められた位置エリアに従って、これらのメッセージをＢＳＣ４に送信する。各セルブロードキャストメッセージには、一意のメッセージ識別子（１６ビット整数）が与えられる。この識別子は、メッセージのタイプを特定する。次に、ＢＳＣ４は、対応するＢＴＳ６を介したそのＣＢＣＨ上でのメッセージ同報に進む。ＣＢＣＨプロトコルおよび同報のタイミングは、ＧＳＭ技術仕様書０５．０２で指定されている。

【００２１】

ＣＢＣ１２は、図３に示されるように、暗号化形式で同報すべきメッセージの各タイプに対して暗号化キーを指定するリストを保持する。このキーは、このようなメッセージの各々について、メッセージ識別子に対してリストされる。各キーは１６ビット整数であり、メッセージ識別子も１６ビット整数であるので、リ

スト内の二つのキーが同一である必要はない。これらのキーは、後述するようにＸＯＲ関数を用いてメッセージを暗号化するために使用される。

【００２２】

図４は、新しい送信用メッセージをセルブロードキャストメッセージとして受け取るときにＣＢＳ１２によって実行される手順を示している。新しいメッセージは、例えばＣＢＣに伴うワークステーション上での手動入力によってＣＢＣ１２内で提供することができ、あるいはリモートソースからオンラインで提供することができる。

【００２３】

ＣＢＣ１２が新しいメッセージ（このメッセージは、同一のメッセージ識別子に対して記憶された前のメッセージを更新したものでもよい）を受信すると、このメッセージは、ＣＢＣ１２によって記憶され、同一のメッセージ識別子に対して記憶された前のメッセージは上書きされる（ステップ５０）。

【００２４】

次に、ＣＢＣ１２は、新しいメッセージが与えられたメッセージ識別子を用いて、図３に示されるキーリストにそのメッセージ識別子が現れているかどうかをチェックする。その特定メッセージ識別子に対してキーが保持されていない場合、このメッセージは、セルブロードキャストによって、メッセージが配信されるセル内でサービスが提供される全ての移動局が一般に利用できるものとなる。このメッセージは、同報通信のために、非暗号化形式で関連ＢＣＳ４に送信される（ステップ５２）。

【００２５】

セルブロードキャストメッセージは、一以上のページ（最大１５ページ）からなる。各セルブロードキャストページは、８８オクテットの情報からなり、この情報は、６オクテットヘッダおよびメッセージテキスト用の８２オクテットからなる。最大９３文字／ページに等しい７ビットデフォルト文字セットが使用される。

【００２６】

図５は、セルブロードキャストメッセージの各ページがＣＢＣＨ上のＢＳＣ／

ＢＴＳによりセル内で伝送される方法を示している。この同報通信は、毎ページあたり４ブロックに分割される。第１のブロック１００には、ページの通し番号を示す２オクテットのデータ１０８、ページのメッセージ識別子を示す２オクテットのデータ１１０、メッセージテキストに使用される符号化方式を特定する１オクテットのデータ１１２、およびページパラメータを示す１オクテットのデータ１１４が含まれる。残りの１６オクテットのデータ１１６には、そのページ用のメッセージテキストの第１の部分が含まれる。

【００２７】

ページ同報の残りの３ブロック１０２、１０４、１０６は、全体的にメッセージテキストからなる。ただし、各ブロックは、ブロックタイプを示す単一オクテットのデータ１１８をヘッダとして含んでいる。

【００２８】

ブロック部分１０８で示される通し番号は、特定のメッセージを識別するために使用される１６ビット整数である。この通し番号は、所定のメッセージ識別子を有するメッセージが更新されるときに更新される。この通し番号は、１２ビットのメッセージコードおよび4ビットの更新番号からなり、これらはメッセージの更新に従って増分される。

【００２９】

部分１１０内のメッセージ識別子は、上述のように、メッセージのタイプを識別するために使用される。

【００３０】

部分１１２に示される符号化方式は、メッセージのソース言語を示すために使用される。これにより、ユーザは、対話不可能な言語で受信されたメッセージを遮断することが可能になる。部分１１４に示されるページパラメータは、メッセージ内の現在のページ番号およびメッセージ内のページ総数を指定するために使用される。

【００３１】

各ページについてのメッセージテキストは、最大９３文字からなる。１ページ内のメッセージテキストの長さが９３文字より短い場合、パッキングを行って文

字総数を９３にするために、復帰（carriage return：ＣＲ）文字が使用される。整数のオクテットを維持するため、残りの５ビットは、ページの終端におけるパディングデータとして「０」に設定される。

【００３２】

図５に示すブロック構造は、従来のセルブロードキャストメッセージの構造である。この構造は、メッセージが同報されるセルブロードキャストチャネルの受信時に、現在利用可能なＧＳＭ型移動局によって受信および表示することができる。

【００３３】

再び図４について説明する。ＣＢＣ１２が、キーリスト内で新しいメッセージのメッセージ識別子を検出すると、対応するキーが検索される（ステップ５４）。次に、このキーを用いてメッセージの暗号化が行われ（ステップ５６）、この後、このメッセージは適切なＢＳＣ４に送信される（ステップ５８）。ステップ５６の暗号化は、次のように行われる。すなわち、キーの最上位８ビットとページ内の各奇数番号メッセージテキストオクテットとの間にＸＯＲ関数を適用し、キーの最下位８ビットとページ内の各偶数番号メッセージテキストオクテット（その最後のオクテットを除く）との間にＸＯＲ関数を適用することによって暗号化が行われる。

【００３４】

暗号化セルブロードキャストメッセージを受信するときにＢＳＣ４により同報されるページは、図６に示される形式を有している。各ページは、図５に示される非暗号化ページと同じ構成要素、すなわち、それぞれ様々なヘッダ部を含む四つのブロックからなる。しかしながら、図６において陰影を付けて示すように、メッセージテキストの大部分は暗号化されている。５ビットのパディングデータを含むメッセージテキストの各ページの最終オクテットは、非暗号化のまま残される。これは、暗号化すると失われてしまうパディングデータの完全性を守るためである。また、各ヘッダ部も非暗号化形式で送信される。これにより、全ての移動局８によるヘッダ部のデータの適切な受信および読取りが可能となる。

【００３５】

暗号化セルブロードキャストメッセージを適切に受信し、理解可能な形式でユーザに提供するためには、メッセージの暗号化に使用された暗号化キーに対応する解読キーを移動局８に与える必要がある。暗号化関数としてＸＯＲ関数を用いると、暗号化／解読プロセスは対称的であり、メッセージの暗号化に使用された同じキーを用いてそのメッセージが解読される。本明細書において、このキーは、データの暗号化に使用される際には暗号化キーと呼ばれ、データの解読に使用される際には解読キーと呼ばれる。

【００３６】

移動局８に解読キーを供給するために、遠隔供給手順が使用される。この手順は、欧州特許出願ＥＰ－Ａ－０５６２８９０（この内容は、参照によって本明細書に組み込まれる）等に記載されているような、移動局８への遠隔ＳＩＭ更新（remote SIM updating：ＲＳＵ）メッセージの送信を含み、あるいはＧＳＭ技術仕様書１１．１４、「Specification of the SIM Application Toolkit for the Subscriber Identity Module - Module Equipment (SIM-ME) Interface」に記載されている「ＳＭＳポイントツーポイント経由データダウンロード」（ＳＭＳ－ＰＰデータダウンロード）手順の使用を含んでいる。解読キーは、ＳＩＭ３４での記憶のために、ＧＳＭ定義ショートメッセージサービス（ＳＭＳ）等のポイントツーポイントデータ転送プロトコルを用いて、無線インタフェース上を移動局８に送信される。ＳＩＭ３４には、セルブロードキャスト解読キーデータの記憶専用のセルブロードキャスト解読キーデータフィールドが設けられる。

【００３７】

図７は、特定加入者がアクセス権を有する各アクセス制限メッセージタイプについての解読キーをその加入者の移動局８に供給するためにＮＭＣ１４によって実行される手順を示している。ＣＳＳ１５は、その加入者についてのアクセス権を示す記録をその加入者に関して保持している。これらのアクセス権は、加入者がアクセスを持つべきメッセージタイプに対する適切なメッセージ識別子のリストを加入者記録の中に含めることによって示される。このアクセス権リストは、ＣＳＳ１５で更新および変更することができる。

【００３８】

加入者の移動局８に供給を行うため、ＮＭＣ１４は、まずＣＳＳ１５に問合せを行い、加入者に対して保持されているメッセージアクセス権を判定する（ステップ６０）。また、ＮＭＣ１４は、加入者のＩＭＳＩを検索するため、ＨＬＲ１１にも問合せを行う（ステップ６２）。更に、ＮＭＣ１４は、ＣＢＣ１２にも問合せを行い、ＣＳＳ１５から返されるアクセス権の詳細のなかで示される各メッセージ識別子に対応する解読キーを検索する（ステップ６４）。次に、ＣＢＣ１２から返される各解読キーは、解読キーの１６ビットと加入者のＩＭＳＩ記録の１６個の所定ビットとの間にＸＯＲ関数を適用することにより、それ自体が暗号化される（ステップ６６）。これは、解読キーを、加入者のＩＭＳＩ（これは、その加入者のＳＩＭ３４に記憶されている）にアクセスする移動局８によってしか使用できないようにするためである。

【００３９】

解読キーが暗号化されると、ＮＭＣ１４は、無線インタフェースを介してＲＳＵメッセージを加入者の移動局８へのＳＭＳメッセージとして送信するために、ＲＳＵメッセージをＳＭＣ１３に転送する。ＳＭＳメッセージは、従来の方法により専用データチャネルを介して移動局８に送信される。ＲＳＵメッセージは、図８に示される形式を有しており、ヘッダ部７０、加入者がアクセスすべき各メッセージタイプに対するメッセージ識別子、暗号化された解読キー、および各メッセージタイプを容易に識別するために加入者によって使用されるアルファタグ（英数字識別子）を含んでいる。ヘッダ部７０は、ＳＭＳメッセージがＲＳＵメッセージであることを示すフラグと、メッセージの内容がセルブロードキャスト解読キーデータフィールドに記憶されるべきことを示すコマンドを含んでいる。

【００４０】

ＳＭＳメッセージを受信すると、移動局は、このメッセージをＳＭＳメッセージとして記憶するためにＳＩＭ３４に転送する。しかしながら、このメッセージはＲＳＵフラグを有するため、ＳＩＭプロセッサ３６はメッセージがＲＳＵメッセージであることに注目し、ＲＳＵメッセージに含まれるメッセージ識別子、対応する暗号化されたキー、および対応するアルファタグを用いて、ＳＩＭ３４内のセルブロードキャスト解読キーデータフィールドを更新する。このようにして

、セルブロードキャスト解読キーデータフィールドに記憶された識別子に対応するメッセージ識別子を有する全ての暗号化されたセルブロードキャストメッセージを解読する能力が移動局に与えられる。

【００４１】

移動局のユーザは、キーパッド３２上で適切にキー操作することにより、ユーザによる表示が可能なように移動局が取得および記憶すべきセルブロードキャストメッセージを選択することができる。また、ユーザは、ユーザが表示を望むアクセス制限メッセージタイプの選択を補助するために、アクセス制限メッセージのメッセージタイプに対するアルファタグを表示させることもできる。更に、ユーザは、一般アクセスメッセージのメッセージタイプに対するメッセージ識別子、および移動局が解読キーを持たないアクセス制限メッセージのメッセージタイプに対するメッセージ識別子も選択することができる。

【００４２】

ユーザによる表示が可能なように選択されるタイプのメッセージ識別子を有するセルブロードキャストメッセージが移動局８によって受信され、そのメッセージ識別子に対して、まだ何らのメッセージも記憶されていない場合、移動局８は、そのメッセージを取得し、ＳＩＭ３４のセルブロードキャストメッセージデータフィールド内に記憶する。ＳＩＭ３４が、セルブロードキャストメッセージ内のメッセージ識別子に対して記憶されたメッセージを既に有している場合、移動局８は、そのメッセージの通し番号をチェックし、更新が行われたかどうかを判断する。更新が行われていれば、移動局は、ＳＩＭ３４内の以前に記憶されたメッセージを更新されたメッセージで上書きする。そうでない場合、移動局８は、セルブロードキャストメッセージの内容を無視する。

【００４３】

セルブロードキャストメッセージが新たに取得および記憶されると、ユーザは、例えば音声により、あるいは移動局８のＬＥＤ表示装置３０上の特定のアイコンにより、セルブロードキャストメッセージの表示の準備ができたことを指示するように促される。次に、移動局は、図９に示される手順を実行する。

【００４４】

移動局は、まず、メッセージの表示を要求するユーザからの入力を待つ。この入力を受信すると、移動局は、自身が現在そのホームネットワーク（ＨＰＬＭＮ）にキャンプオンされているかどうかをチェックする。移動局がそのホームネットワークではないネットワークにキャンプオンされていると、移動局は、記憶されたメッセージの表示に直接進む。そのメッセージが暗号化されている場合、その暗号化メッセージは、ユーザが理解不可能な形で表示される（ステップ７８）。これは、そのメッセージがアクセス制限タイプのメッセージであり、他のネットワーク加入者には、その情報へのアクセスが許可されないからである。しかしながら、メッセージが暗合化されていない場合、すなわちメッセージが一般アクセスタイプのメッセージである場合、そのメッセージは、理解可能な形で表示される（ステップ８０）。

【００４５】

移動局が、そのホームネットワークにキャンプオンされている場合、移動局は、本発明にしたがって供給されたセルブロードキャスト解読キーデータフィールドをＳＩＭ３４が有しているかどうかをチェックする。セルブロードキャスト解読キーデータフィールドを有していない場合、移動局は、メッセージ同報のアクセスタイプに応じて、もう一度暗号化メッセージの表示に進むか（ステップ７８）、理解可能なメッセージの表示（ステップ８０）に進む。

【００４６】

現在移動局内に位置するＳＩＭ３４がセルブロードキャスト解読キーデータフィールドを有する場合、移動局は、ＳＩＭ３４への問合せに進み、記憶されたメッセージのメッセージ識別子がセルブロードキャスト解読キーデータフィールドに存在するかどうかをチェックする。存在しない場合、受信メッセージは一般アクセスタイプのメッセージであり、このメッセージは、理解可能な形で移動局８により表示される（ステップ８０）。そうでない場合、このメッセージは、ユーザがアクセス権を持たないアクセス制限タイプのメッセージである。この場合、メッセージは、暗号化された形、すなわち理解不可能な形で移動局８により表示され、これにより、ユーザによるそのメッセージ内の情報の受け取りが防止される（ステップ７８）。

【００４７】

記憶されたメッセージのメッセージ識別子がＳＩＭ３４上のセルブロードキャスト解読キーデータフィールドに存在する場合、移動局８は、記憶メッセージのメッセージ識別子に対応する被暗号化解読キーを加入者のＩＭＳＩと共にＳＩＭから検索する工程に進む（ステップ８２）。

【００４８】

被暗号化解読キーとＩＭＳＩを用いることにより、移動局８は、ＮＭＣ１４で行われる暗号化処理とは逆の処理を実行し、元の解読キーを得る（ステップ８４）。この解読は、１６ビットの被暗号化解読キーと、暗号化プロセスで使用された加入者ＩＭＳＩからの所定１６ビットからなる同一セットとの間でＸＯＲ関数を実行することにより行われる。

【００４９】

次に、移動局８は、記憶メッセージの解読に進む。この解読は、暗号化セルブロードキャストメッセージの作成時にＣＢＣ１２で行われた暗号化処理と逆の処理を実行することにより行われる。すなわち、移動局は、解読キーの８個の最上位ビットと各奇数番号メッセージテキストオクテットとの間でＸＯＲ関数を実行するとともに、解読キーの８個の最下位ビットと各偶数番号メッセージテキストオクテット（各ページ内の最終オクテット（もともと暗号化されなかった）を除く）との間でＸＯＲ関数を実行する。これにより、元のセルブロードキャストメッセージテキストが復元され、この後、このメッセージテキストは、ユーザが理解可能な形で移動局のＬＣＤ表示装置３０上に表示される（ステップ８８）。

【００５０】

図１０は、８９個のメッセージテキスト文字および４個の復帰（テキストパディング）文字からなるオリジナルセルブロードキャストメッセージの一例を示している。このメッセージは、図４を参照して説明したように暗号化され、移動局によって受信及び記憶された後は、図９に示される手順に従って表示することができる。

【００５１】

対応する解読キーが移動局に与えられている場合、このメッセージは、図１０

に示されるように元の形で表示される。

【００５２】

一方、移動局に適切な解読キーが与えられていない場合、このメッセージは、図１１に示されるように擬似ランダム文字セットとして現れる。

【００５３】

暗号化キーのビット数は、テキストの符号化において各文字ごとに使用されるビット数に等しくもなければ、その倍数でもないので、元の文字の任意の一つと暗号化されたテキスト内に表示される文字との間に直接の対応はない。この場合、テキスト文字に使用される符号化方式は１文字あたり７ビットを使用し、暗号化キーは１６ビットを含んでいる。もちろん、テキスト文字符号化長と暗号化キー長の他の組合せを用いても同様の効果を得ることができる。

【００５４】

アクセス制限メッセージに使用される暗号化方法の長期安全性を確保するためには、メッセージテキストを暗号化するために使用される暗号化キーが定期的に変更されることになる。図１２は、特定の暗号化キーを更新するためにＣＢＣ１２によって実行される手順を示している。ＣＢＣ１２は、まず、新しい１６ビット暗号化キーをランダムに生成し（ステップ９０）、次いで、対象のメッセージ識別子に対して図３に示されるリスト内に以前に記憶された暗号化キーを上書きする（ステップ９１）。次に、ＣＢＣ１２は、対象の識別子に対して以前に記憶されたメッセージを検索する工程に進み（ステップ９２）、次いで、そのメッセージを新しく生成された暗号化キーで暗号化する工程に進む（ステップ９３）。この暗号化処理は、図４を参照して説明したようにメッセージがＣＢＣ１２によって初めに受信された時に実行されたものと同一であるが、もちろん異なる暗号化キーを使用する。メッセージが暗号化されると、新しいセルブロードキャストメッセージが適切なＢＳＣ４に転送される（ステップ９４）。これは、ＢＴＳ６が、対象のＢＳＣ４によってサービスが提供されるセル中のセルブロードキャストチャネルを受信する移動局８に向けてＣＢＣＨ上で同報を行うためである。

【００５５】

新しい暗号化キーがＣＢＣ１２で生成され、対応するセルブロードキャストメ

ッセージが新しく生成されたキーを用いて暗号化されると、同じメッセージタイプへのアクセス権を有するユーザの移動局８に新しい解読キーを与えなければならなくなる。

【００５６】

適切な加入者の移動局８にＣＢＣ１２で生成された新しい解読キーを供給する第１のステップは、図１３のように実行される手順である。まず、ＣＳＳ１５は、解読キーが更新されたメッセージのメッセージ識別子のリストをＣＢＣ１２から受信する（ステップ９５）。次に、ＣＳＳ１５は、更新された解読キーリスト上のメッセージ識別子に対する加入記録の記憶を探索する工程に進む（ステップ９６）。これは、どの加入契約が更新された解読キーを必要とするかを判断するためである。次いで、ＣＳＳ１２は、このような加入契約のリストを構築する。これらの加入契約はＮＭＣ１４に転送され、これにより、ＮＭＣ１４が適切な供給手順を実行できるようになる（ステップ９７）。この後、ＮＭＣ１４は、ＣＳＳ１５から受信したリストに現れる各加入契約に関して、図７を参照して説明した手順を実行する工程に進む。その結果、このような各加入契約の移動局は、その加入者がアクセスするメッセージタイプに対して、更新された解読キーを含む新しいＲＳＵメッセージを暗号化された形式で受信することになる。これらの解読キーは、新たに生成された暗号化キーを用いて暗号化されたメッセージの解読時に使用するのに適している。

【００５７】

上述の実施形態で利用される暗号化／解読機構は、ＸＯＲ関数の両方向暗号化／解読文字を利用するものであり、多くの種類の情報に関連して使用するにあたって十分に安全である。しかしながら、他の両方向暗号化／解読機構（例えば、対称暗号化／解読キーや公衆／専用の暗号化／解読キーを用いるもの）を利用して、より安全度の高い（あるいは低い）暗号化／解読機構を提供してもよい。

【００５８】

上述の実施形態では、一般アクセスメッセージには、暗号化／解読プロセスで使用されるＸＯＲ関数は適用されない。しかしながら、「０」の１６ビットからなる形の「自由」キーを用いて、このメッセージにＸＯＲ関数を適用することも

可能である。この結果、元のメッセージ符号化と同一のメッセージ符号化が行われる。「自由」キーを用いたＸＯＲ実行は、一般アクセスメッセージの「暗号化」の際にＣＢＣ１２で行われ、かつ／または一般アクセスメッセージの「解読」の際に移動局８によって行われてもよい。実際には、暗号化または解読は行われない。

【００５９】

上述の実施形態では、移動局８がセルブロードキャストメッセージテキストの解読を実行する。これには、現存する移動局タイプに関連して、移動局自体をカスタマイズする必要がある。これは、移動局が、暗号化されたセルブロードキャストメッセージを普通テキスト形式で提供できるようにするためである。別の実施形態では、ＧＳＭ技術仕様書１１．１４に記載されているようなＳＩＭツールキットをサポートするＧＳＭ（フェーズ２＋）移動局などの標準移動局を使用してもよい。この実施形態では、暗号化されたセルブロードキャストメッセージを解読する機能がＳＩＭ３４自体に含まれている。このＳＩＭ３４は、ＳＩＭツールキットにより使用可能とされる。

【００６０】

繰返しを避けるため、図３、４、７、８、１２および１３の各々に関して説明した機能は、図１３に関して等しく適用するものとする。本実施形態は、最初に述べた実施形態と主に次の点で異なる。すなわち、図６に示される特別なセルブロードキャスト符号化方式は必要でなく、その代わりに従来の「ＳＭＳ－ＣＢ経由データダウンロード」符号化方式が使用される。また、図９に示される手順が移動局によって実行されず、その代わりに移動局は、「ＳＭＳ－ＣＢ経由データダウンロード」メッセージをＳＩＭに直接引き渡し、続いて、ＳＩＭ（このＳＩＭはプロアクティブである）の指示により、暗号化形式で受信したセルブロードキャストメッセージの普通テキストバージョンを表示する。

【００６１】

図４に関して、この実施形態では、任意の適切な種類の暗号化技術をステップ５６で使用することができる。これは、前述のＸＯＲ関数であってもよいし、ＤＥＳ、ＲＳＡ等、他の暗号化技術であってもよい。

【００６２】

図６に示される符号化方式の代わりに、本実施形態では、暗号化されたセルブロードキャストメッセージを同報するＢＳＣ４の各々が、その暗号化メッセージを「ＳＭＳ－ＣＢ経由データダウンロード」メッセージとしてフォーマットする。この暗号化メッセージは、そのメッセージの暗号化に使用されたキー用の識別子と共にセルブロードキャストページに含まれる。セルブロードキャストメッセージは、セルブロードキャストページに含まれる内容の種類を指定するセルブロードキャストメッセージ識別子と、メッセージタイプが「ＳＩＭデータダウンロード」であることを示す転送識別子とを含む。

【００６３】

解読キー専用のフィールド（これは、上述したようなＲＳＵ手順によって埋められる）に加え、ＳＩＭ３４は、ＧＳＭ技術仕様書１１．１１に記載されるようなデータダウンロード用セルブロードキャスト識別子（Cell Broadcast Message Identity for Data Download：ＣＢＭＩＤ）データフィールドを含んでいる。このデータフィールドは、加入者がその移動局８で受け取りたいと考えるメッセージ内容タイプを識別するデータを保持する。更に、ＳＩＭ３４には、解読と移動局８の表示装置の制御を実行するアプリケーションプログラムも含まれる。このアプリケーションプログラムは、例えば、ＳＩＭ上のＲＯＭまたはＥＥＰＲＯＭに格納することができる。

【００６４】

移動局がセルブロードキャストダウンロードメッセージを受信すると、移動局８は、まずＳＩＭのＣＢＭＩＤデータフィールドに問合せを行い、セルブロードキャストメッセージに関して受信されたメッセージＩＤが、加入者によって、または加入者のために現在選択されているかどうかを判断する。対応するエントリがＣＢＭＩＤデータフィールド内で発見されると、移動局８は、「ＳＩＭへのセルブロードキャストダウンロード」コマンドを用いてＳＩＭ３４にセルブロードキャストページを透過的に引き渡す。

【００６５】

ＳＩＭ３４がセルブロードキャストダウンロードコマンドを受け取ると、ＳＩ

Ｍは、セルブロードキャストページの少なくとも一部の内容を分析することになる。これにより、セルブロードキャストページが暗号化されたメッセージを含んでいるかどうかが判断される。暗号化メッセージを含んでいる場合、専用解読キーフィールドに記憶された適切な解読キーを用いてメッセージを解読するために、記憶プログラムが呼び出される。メッセージが解読されると、ＳＩＭは、その普通テキストメッセージを「テキスト表示」コマンドで移動局に引き渡す。これに応じて、移動局８は、その普通テキストメッセージを表示する。

【００６６】

暗号化メッセージの解読および移動局８に指令して普通テキストメッセージを表示させることに加えて、ＳＩＭアプリケーションプログラムは、セルブロードキャストメッセージ中で受信したデータに応じで他の処理を実行してもよい。この処理としては、例えば、ＣＢＭＩＤデータフィールドの内容を更新し、移動局８が受信および処理すべき新しいメッセージ種類を加入者に代わって選択することなどが挙げられる。

【００６７】

本実施形態では、加入者が普通テキスト形式のアクセス制限メッセージの受信を許可されていない場合、ＳＩＭは、このメッセージ用の適切な解読キーを含んでいなくてもよいし、あるいはネットワークオペレータによって少なくとも一時的に、上記手順を実行しないように構成されていてもよい。上記手順の代わりに、ＳＩＭは、様々な別の方法において機能することができる。例えば、ＳＩＭが移動局８に指令を出して、メッセージを暗号化形式でユーザに提供させ、またはアクセス拒否メッセージを表示させてもよいし、それでもなお加入者によって選択される種類の暗号化メッセージを含むセルブロードキャストメッセージに応答して、単純に移動局上にいかなる表示も行わないようにしてもよい。

【００６８】

従って、暗号化セルブロードキャストメッセージの供給および処理機能は、移動体通信ネットワーク内およびＳＩＭ３４上に完全に含めることができ、標準（例えば、ＧＳＭフェース２＋）ハンドセットを改造なしで使用することができる。

【００６９】

上記実施形態に関しては、様々な修正および変形を加えることができる。

【００７０】

ＲＳＵタイプのショートメッセージを用いて、移動局にエアインタフェースを介して解読キーを供給することは、以下の点で有効である。すなわち、移動局８のＳＩＭ３４に解読キーを供給するにあたって、加入者側では何らの動作も必要ないことである。しかしながら、解読キー（好ましくは、上述のように加入者のＩＭＳＩ等を用いて暗号化されたもの）を他の方法（例えば、郵送）でユーザに送ってもよい。移動局８の他の機能により、暗号化された解読キーを手動で移動局に入力し、ＳＩＭ３４内のセルブロードキャスト解読キーデータフィールドに記憶することが可能になる。

【００７１】

前記の機構に代わって、他の情報アクセス防止機構を使用することもできる。例えば、移動局上の解読機能や移動局上のセルブロードキャスト受信機能の遠隔許可／禁止が挙げられる。

【００７２】

上記実施形態において、ＳＩＭ３４は、移動局８に電気接続されたモジュールの形態をとっている。しかし、ＳＩＭは、無線リンクを介して移動局との間でデータ伝送を行う非接触スマートカードなど、全く独立のモジュールとして実現してもよい。

【００７３】

最後に、上記実施形態は、ＧＳＭタイプのネットワークで利用される方法および装置に関するものであるが、ＴＤＭＡ、ＣＤＭＡ、または他の種類の無線インタフェースプロトコルを使用して、他の種類のセルラー方式電気通信ネットワークで本発明を実現できることは言うまでもない。

【００７４】

本発明の範囲から逸脱することなく、更なる修正や変形を加えることが可能である。

【図面の簡単な説明】

【図１】

セルラー方式電気通信システムを概略的に示すブロック図である。

【図２】

セルラー方式電気通信移動局を概略的に示すブロック図である。

【図３】

本発明に係るセルブロードキャストセンタに記憶されたリストを示す図である。

【図４】

本発明に係るセルブロードキャストセンタが実行する機能を示すフローチャートである。

【図５】

本発明に係るセル内のデータブロック同報通信を示す図である。

【図６】

本発明に係るセル内のデータブロック同報通信を示す図である。

【図７】

本発明に係るネットワーク管理センタが実行する機能を示すフローチャートである。

【図８】

本発明に係る移動局に送信されるショートメッセージを示す図である。

【図９】

本発明に係るセルブロードキャストメッセージを表示する時に移動局が実行する機能を示す図である。

【図１０】

本発明に係る解読メッセージの表示例を示す図である。

【図１１】

本発明に係る暗号化メッセージの表示例を示す図である。

【図１２】

本発明に従って実行される暗号化キー更新手順を示すフローチャートである。

【図１３】

本発明に従って実行される暗号化キー更新手順を示すフローチャートである。

【図１】

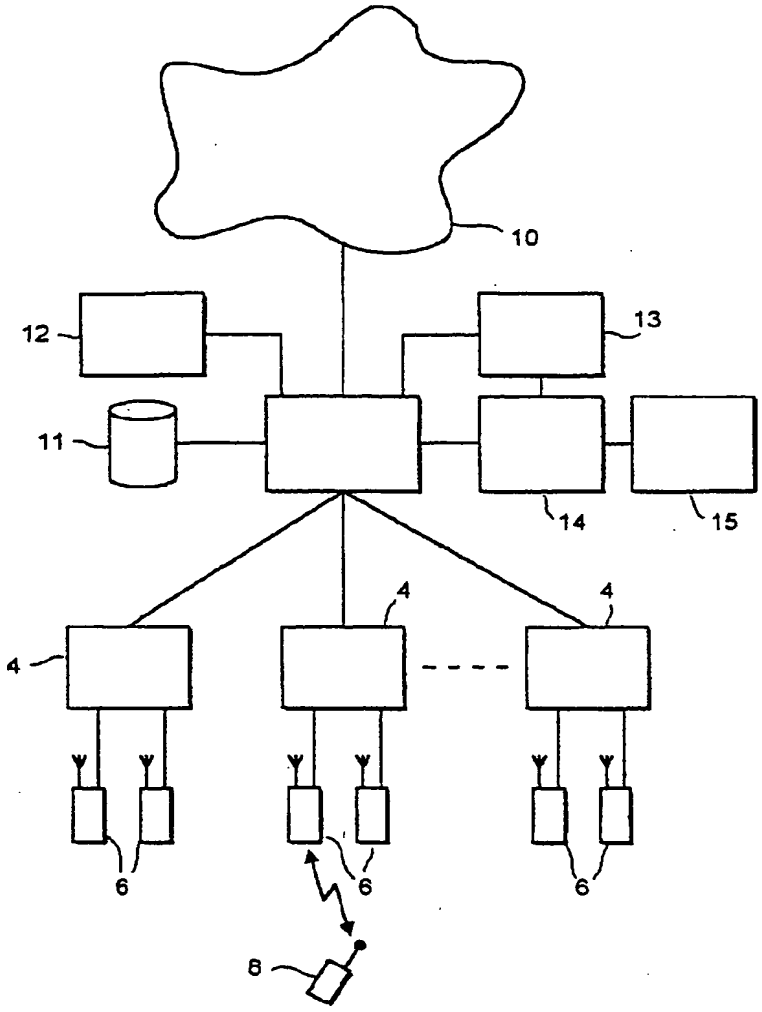


FIG. 1

【図２】

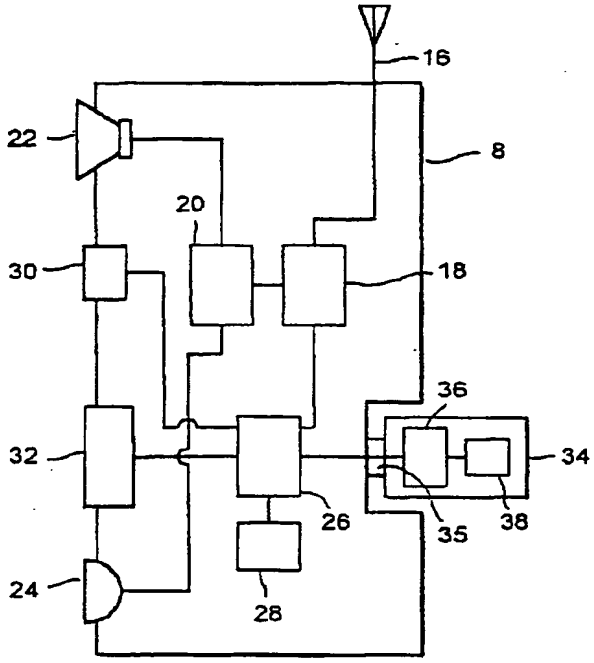
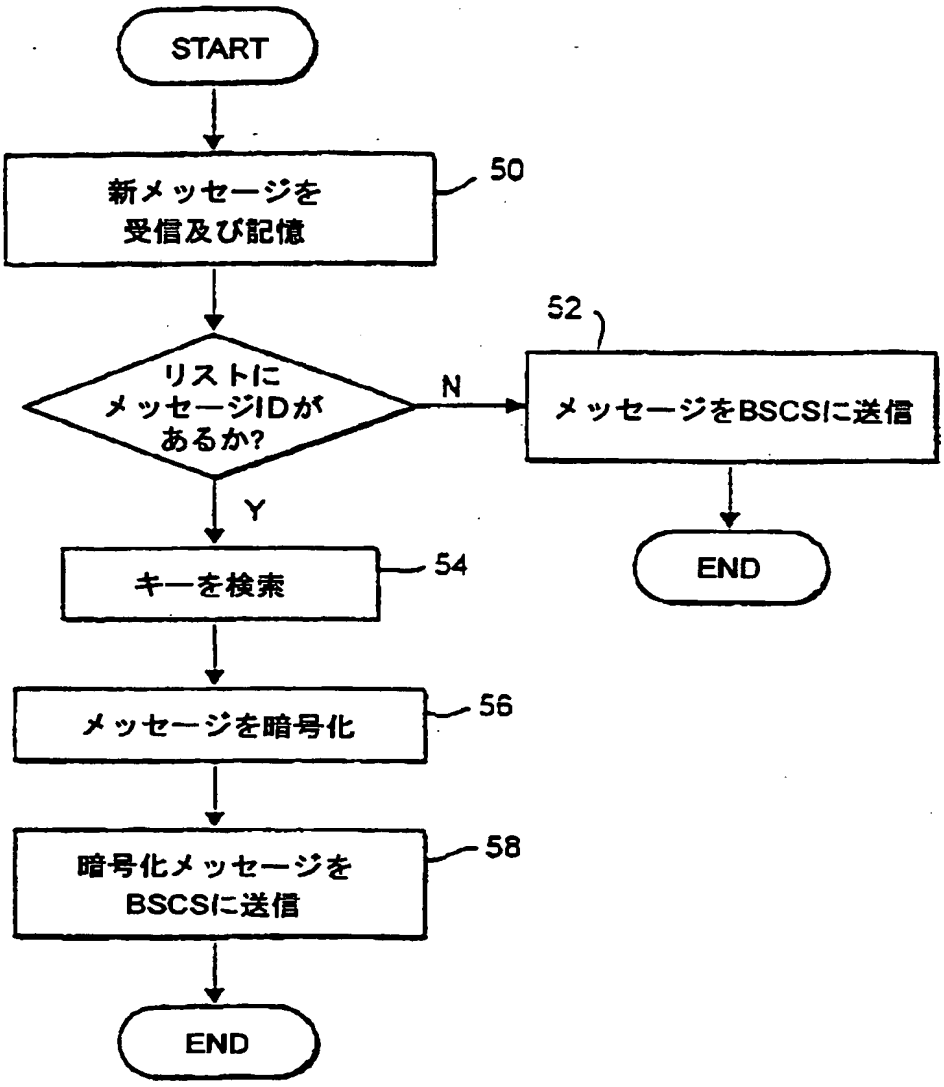


FIG. 2

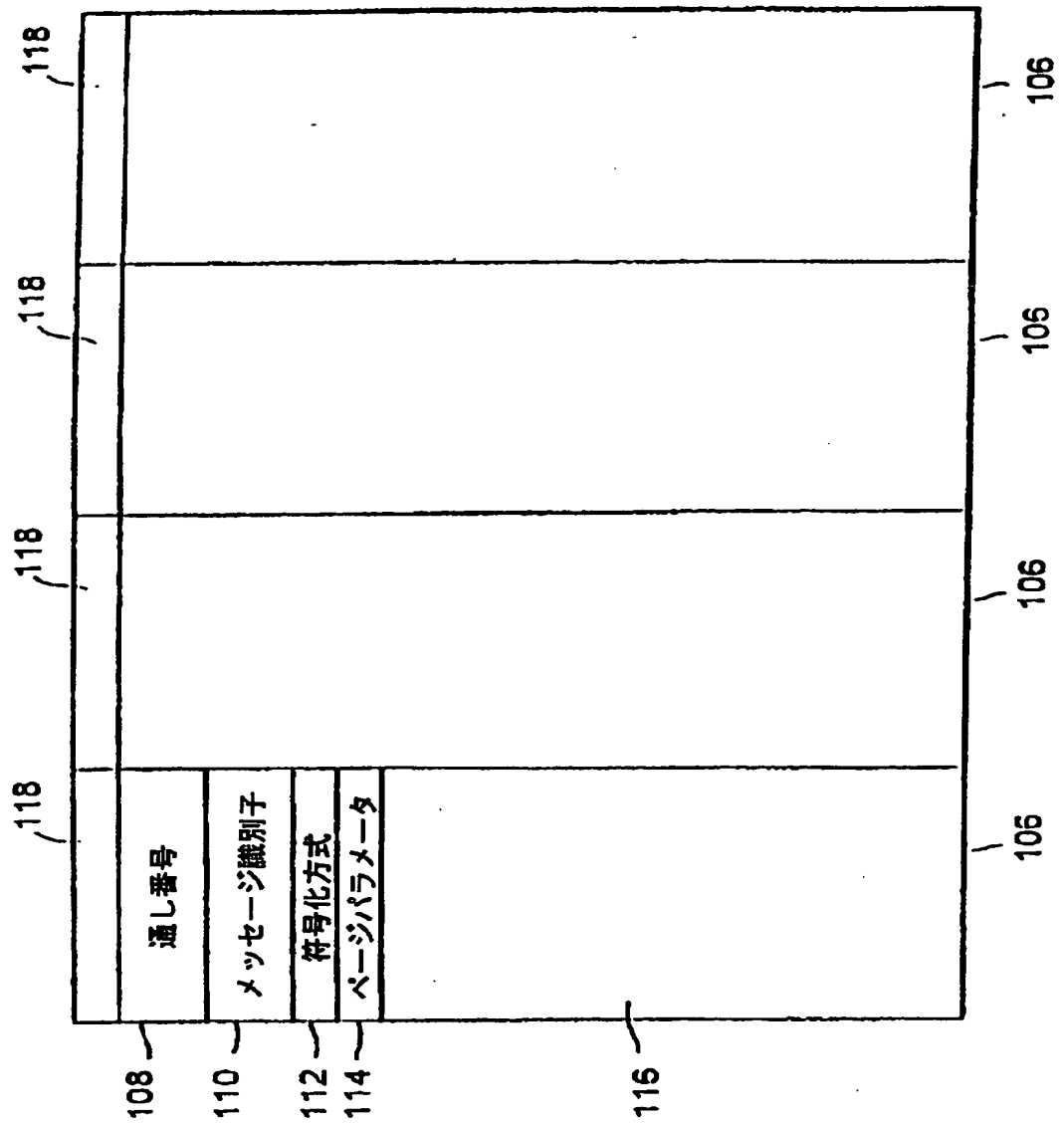
【図３】

メッセージ識別子	キー
----------	----------
----------	----------
• • •	• • •
----------	----------

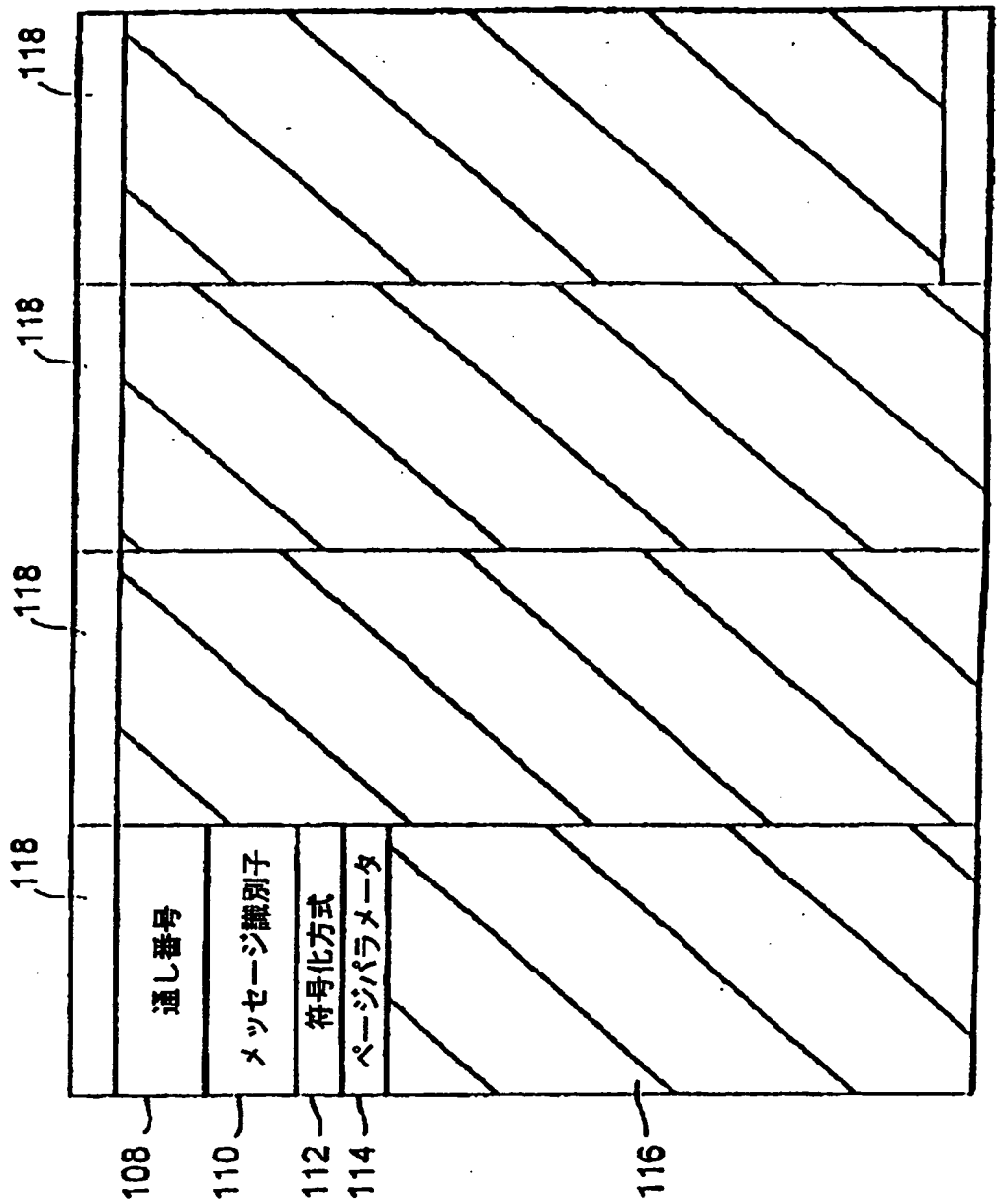
【図４】


START
新メッセージを
受信及び記憶
50
リストに
メッセージIDが
あるか?
N
52
メッセージをBSCSに送信
END
Y
キーを検索
54
メッセージを暗号化
56
暗号化メッセージを
BSCSに送信
58
END

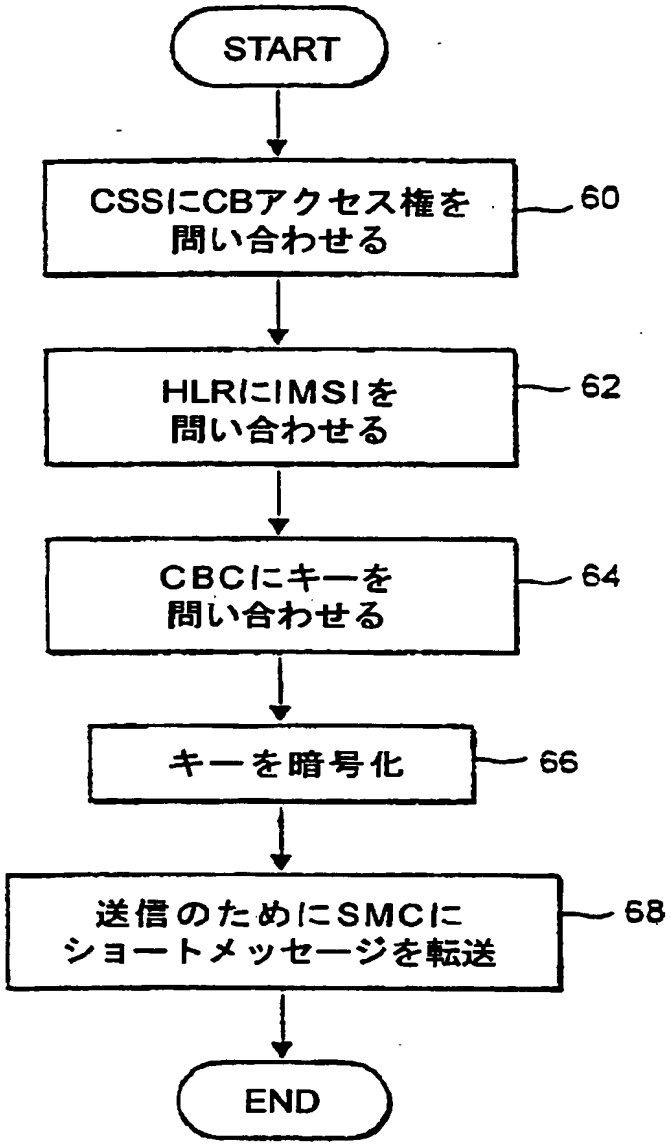
【図５】



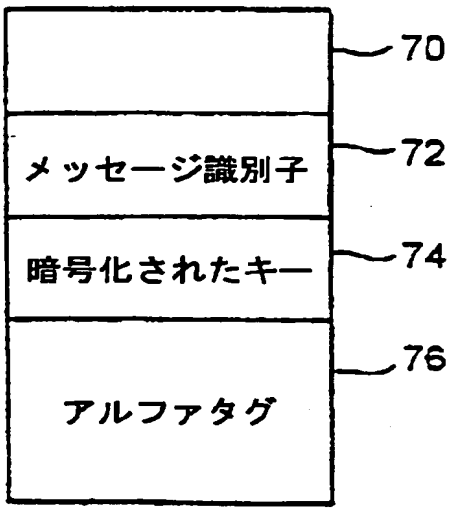
【図６】


118
118
118
118
通し番号
メッセージ識別子
符号化方式
ページパラメータ
108
110
112
114
116

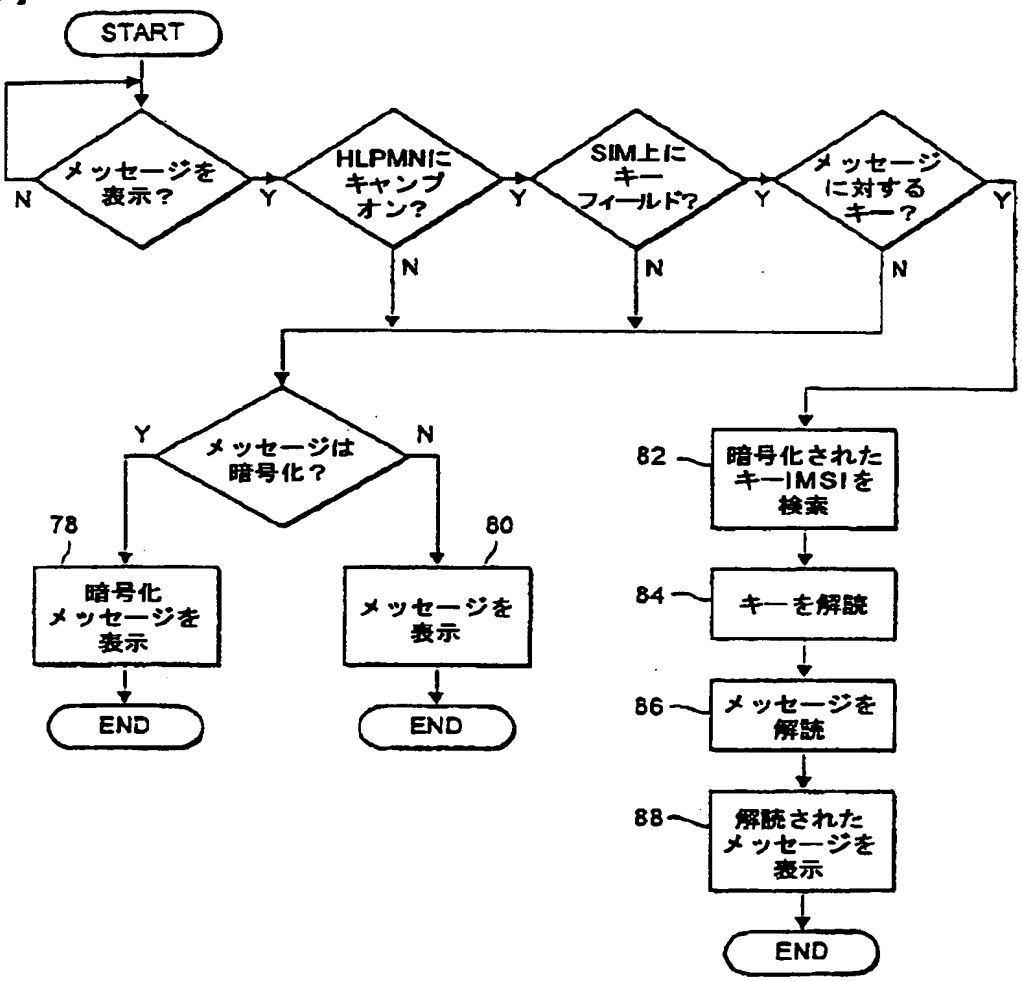
【図７】


START
CSSにCBアクセス権を問い合わせる
60
HLRにIMSIを問い合わせる
62
CBCにキーを問い合わせる
64
キーを暗号化
66
送信のためにSMCにショートメッセージを転送
68
END

【図８】


70
メッセージ識別子
72
暗号化されたキー
74
アルファタグ
76

【図９】


START
メッセージを表示？
N
Y
HLPMNにキャンプオン？
Y
N
SIM上にキーフィールド？
Y
N
メッセージに対するキー？
Y
N
メッセージは暗号化？
Y
N
78
暗号化メッセージを表示
END
80
メッセージを表示
END
82
暗号化されたキーIMSIを検索
84
キーを解読
86
メッセージを解読
88
解読されたメッセージを表示
END

【図１０】

T	h	i	s		i	s		a	n		e	x	a	m	p	l	e		o	f		h	o	w		S	M	S	
C	B		m	e	s	s	a	g	e	s		s	h	a	l	l		b	e		c	o	d	e	d	.	C	a	l
l		"	0	4	5	4	6	2	4	8	2	3	"		F	o	r		m	o	r	e		i	n	f	o	.	CR
CR	CR	CR																											

FIG. 10

【図１１】

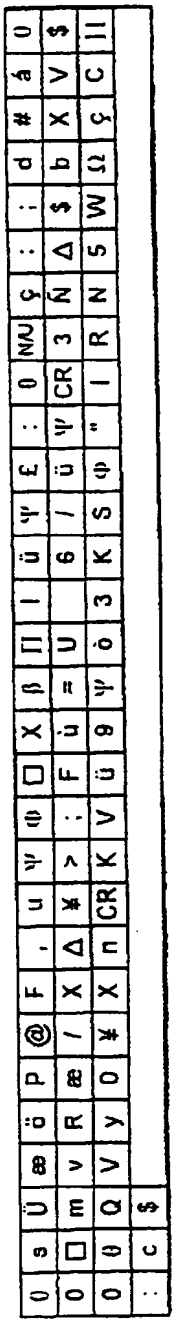
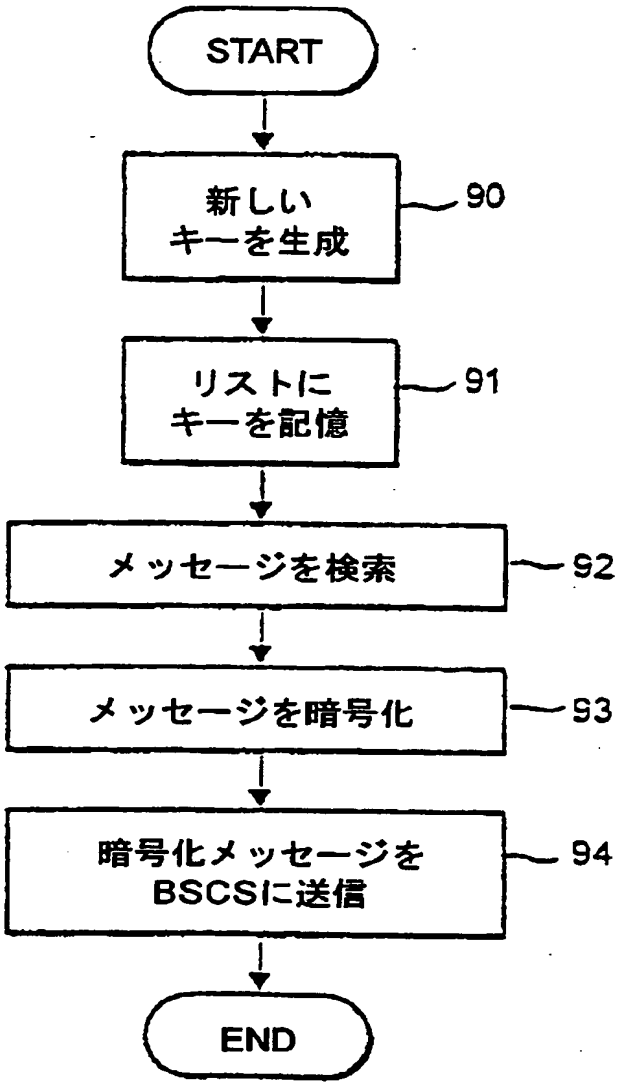
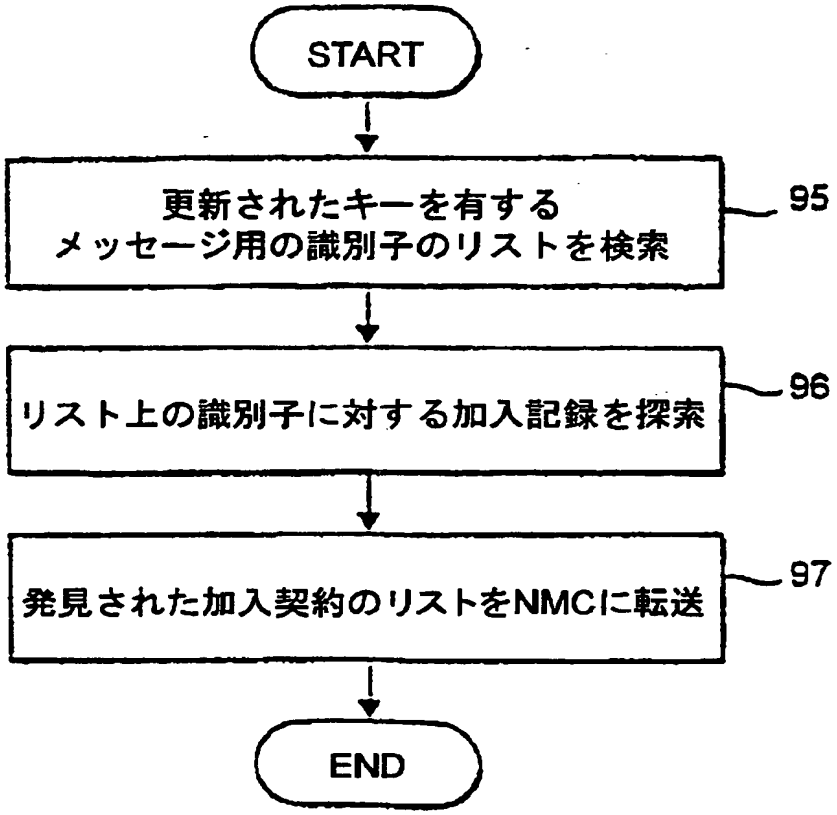


FIG. 11

【図１２】


START
新しい
キーを生成
90
リストに
キーを記憶
91
メッセージを検索
92
メッセージを暗号化
93
暗号化メッセージを
BSCSに送信
94
END

【図１３】


START
更新されたキーを有する
メッセージ用の識別子のリストを検索
95
リスト上の識別子に対する加入記録を探索
96
発見された加入契約のリストをNMCに転送
97
END

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1,2,6, 13-16, 18-21,25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10	3,7,8, 12,17,22
	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 November 1998	18/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Baas, G

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 98/02064

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9641493 A	19-12-1996	US 5768276 A	16-06-1998
		AU 6020296 A	30-12-1996
US 5371493 A	06-12-1994	DE 69219991 D	03-07-1997
		DE 69219991 T	27-11-1997
		EP 0538933 A	28-04-1993
		JP 5218946 A	27-08-1993
		SG 48347 A	17-04-1998
EP 0689368 A	27-12-1995	AT 153206 T	15-05-1997
		AU 691271 B	14-05-1998
		AU 2174595 A	04-01-1996
		BR 9508091 A	12-08-1997
		CA 2152215 A	21-12-1995
		WO 9535635 A	28-12-1995
		CN 1128476 A	07-08-1996
		CZ 9603513 A	14-05-1997
		DE 59402759 D	19-06-1997
		DK 689368 T	08-12-1997
		ES 2103557 T	16-09-1997
		FI 965078 A	17-12-1996
		GR 3023908 T	30-09-1997
		HU 76397 A	28-08-1997
		JP 8265843 A	11-10-1996
		NO 965315 A	18-02-1997
		NZ 287390 A	19-12-1997
		PL 317643 A	14-04-1997
		SG 34235 A	06-12-1996
		SI 9520064 A	30-04-1997
		SK 161396 A	05-11-1997
		ZA 9505091 A	10-04-1996

フロントページの続き

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
H04Q 7/24		H04Q 7/04	A	
7/26				
7/30				

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

Fターム(参考) 5J104 AA16 BA03 EA06 EA18 JA03 NA01 NA02 NA36 NA41
5K067 AA00 BB04 CC04 CC14 DD17 EE16 EE22 HH21 HH36 KK13 KK15